UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Six Electronic Devices, as described in Attachment A

Case No. **21 MAG 5417**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Six Electronic Devices, as described in Attachment A

located in the Southern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1343 and 2,15 U.S.C. Sections 78j(b) & 78ff, 17 C.F.R. Section 240.10b-5	Wire Fraud, Securities Fraud, Aiding and Abetting

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

S/by the Court with permission
Applicant's signature

Edward F. Gannon, Postal Inspector, USPIS
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone *(specify reliable electronic means).*

Date: 05/21/2021

Judge's signature

City and state: New York, New York

Hon. Robert W. Lehrburger, U.S. Magistrate Judge
Printed name and title

Print Save As... Attach Reset

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

21 MAG 5417

In the Matter of the Application of the United States of America for a Search and Seizure Warrant for Six Electronic Devices, USAO Reference No. 2020R01321

TO BE FILED UNDER SEAL

Agent Affidavit in Support of Application for Search and Seizure Warrant

SOUTHERN DISTRICT OF NEW YORK) ss.:

EDWARD F. GANNON, being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I have been a Postal Inspector with the United States Postal Inspection Service ("USPIS") for approximately 14 years. As a Postal Inspector, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. During my tenure with USPIS, I have participated in the investigations of numerous frauds, and have conducted physical and electronic surveillance, the execution of search warrants, and debriefing of witnesses. Through my training, education, and experience, I have become familiar with the manner in which securities frauds are perpetrated.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic devices specified below (the "Subject Devices") for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of cellphones in criminal activity and the forensic analysis of

electronically stored information ("ESI"). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Devices

3. The Subject Devices are particularly described as:

a. A silver Apple MacBook Pro with serial number C02VJ3RAG8WN ("Subject Device-1");

b. An Apple iPhone 11 Pro Max space gray in color ("Subject Device-2");

c. An Apple iPhone and Box with power cord ("Subject Device-3");

d. A 4 terabyte G Drive Hard drive with serial number WX11D79FHD7U ("Subject Device-4");

e. A 2 terabyte G Drive Hard drive with serial number WX11E29C1N68 ("Subject Device-5");

f. An Apple MacBook Air with serial number C1MPWM68G940 ("Subject Device-6" and, collectively, with Subject Device-1 through 5, the "Subject Devices").

4. Based on my training, experience, and research, I know that Subject Device-2 and Subject Device-3 have capabilities that allow them to serve as, among other things, a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. Subject Device-1, Subject Device-4, Subject Device-5, and Subject Device-6 have the capability to store electronic data, including documents and photographs.

5. The Subject Devices are presently located in the Southern District of New York.

C. The Subject Offenses

6. For the reasons detailed below, there is probable cause to believe that the Subject Devices contain evidence, fruits, and instrumentalities of violations of Title 15, United States Code, Sections 78j(b) & 78ff, 17 C.F.R. Section 240.10b-5 (securities fraud); and Title 18, United States Code, Sections 1343 (wire fraud) and 2 (aiding and abetting) (collectively, the "Subject Offenses").

II. Probable Cause Regarding the Commission of the Subject Offenses

7. On April 20, 2021, ANDREW FRANZONE was charged in a Complaint captioned *United States v. Andrew Franzone*, with violations of the Subject Offenses from in or about 2014 through in or about September 2019. The aforementioned Complaint (the "Complaint') is attached hereto as Exhibit A and incorporated by reference in this Affidavit. On April 20, 2021 the Honorable James L. Cott, United States Magistrate Judge, Southern District of New York, signed an arrest warrant for FRANZONE.

III. Probable Cause Regarding the Subject Devices

8. As detailed in the Complaint, ANDREW FRANZONE was formerly the General Partner of FF Fund I L.P. ("FF Fund"), an investment fund currently in liquidation proceedings in the Southern District of Florida (the "Fund Liquidation"). During an April 16, 2021 deposition in the course of the Fund Liquidation, FRANZONE indicated that he did not have a permanent residence address at that time.

9. On or about April 20, 2021, the Honorable James L. Cott, United States Magistrate Judge, Southern District of New York, signed a warrant authorizing USPIS to obtain prospective geolocation data for a phone used by FRANZONE (the "GPS Warrant"). Based upon my review of data obtained pursuant to the GPS Warrant, I concluded that FRANZONE

was likely residing in the vicinity of a hotel located at 321 N. Ft Lauderdale Beach Blvd., Fort Lauderdale, Florida 33304 (the "Hotel").

10. On or about April 22, 2021, I spoke with a manager of the Hotel, who told me, in substance and in part, that FRANZONE had been living at the Hotel for approximately the previous 12 months, but was slated to leave the hotel that day due to nonpayment. Based upon my review of records provided by the Hotel, I have learned that FRANZONE was a guest at the Hotel continuously from in or about April 2020 until on or about April 22, 2021, and that the Subject Premises was FRANZONE's room from at least in or about December 2020 until on or about April 22, 2021.

11. On or about April 22, 2021, FRANZONE was arrested at a restaurant on the Hotel premises. At the time of his arrest, FRANZONE was in possession of Subject Device-1 and Subject Device-2. I took possession of Subject Device-1 and Subject Device-2 at the time of FRANZONE's arrest.

12. On or about April 28, 2021, another representative of the Hotel ("Hotel Employee-1") told me that Hotel Employee-1 had entered FRANZONE's hotel room (the "Hotel Room") the previous day at the request of a member of FRANZONE's family to collect FRANZONE's belongings. When Hotel Employee-1 was inside the Hotel Room, Hotel Employee-1 observed a laptop computer and what appeared to be piles of financial documents.

13. Based upon my conversations with Hotel Employee-1 on or about April 30, 2021, I understood that FRANZONE's belongings remained in the Hotel Room. On that date, based in part on the foregoing, the Honorable Lurana S. Snow, United States Magistrate Judge, Southern District of Florida, signed a warrant authorizing the search of the Hotel Room, as well as the contents of any electronic devices found therein (the "Hotel Room Warrant").

14. On or about May 1, 2021, I served Hotel Empoyee-1 with the Hotel Room Warrant. Upon receipt of the Hotel Room Warrant, Hotel Employee-1 told me that FRANZONE's belongings (the "Franzone Evidence") had been removed from the Hotel Room and were secured in the Hotel, but that Hotel Employee-1 would provide the Franzone Evidence to USPIS based upon the Hotel Room Warrant. On or about May 3, 2021, another Postal Inspector with USPIS ("Postal Inspector-1") went to the Hotel to pick up the Franzone Evidence. Postal Inspector-1 subsequently arranged for the Franzone Evidence to be shipped to me. Based upon my review of the Franzone Evidence, I have learned that the Franzone Evidence contains financial documents, documents related to the Fund Liquidation, credit cards, and several electronic devices, including but not limited Subject Device-3, Subject Device-4, Subject Device-5 and Subject Device-6.

15. Based on my training and experience, I know that individuals who engage in conspiracies to commit wire fraud and securities fraud, commonly use computers, cellphones, and other electronic devices such as the Subject Devices to access websites used for illegal activity; communicate with co-conspirators and victims online; keep track of co-conspirators' and victims' contact information; keep a record of illegal transactions or criminal proceeds for future reference; store data regarding victims and potential victims for future exploitation. As a result, they often store data on their computers, cellphones, and other electronic devices related to their illegal activity, which can include logs of online "chats" with co-conspirators or victims; email correspondence; contact information of co-conspirators and victims, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts; financial and personal identification data for victims and potential victims, including bank account numbers,

credit card numbers, and names, addresses, and telephone numbers of other individuals; and/or records of illegal transactions or the disposition of criminal proceeds.

16. Based upon my participation in this investigation and my review of email communications involving FRANZONE, and as set forth in Exhibit A, ¶¶ 5-7, I know that FRANZONE used email to communicate with investors in FF Fund to perpetrate the Subject Offenses. Specifically, FRANZONE sent victims of the FF Fund scheme monthly "performance reports" attached to email communications. *Id.* ¶¶ 5(e), 6(e).

17. Based upon my participation in this investigation, including my interviews of Wealth Manager-1 and my review of materials provided by Wealth Manager-1, I know that FRANZONE communicated regarding FF Fund via text message. Specifically, following the April 30, 2019 meeting at which Wealth Manager-1 confronted FRANZONE about the liquidity of FF Fund and demanded audited financial statements (*see* Exhibit A ¶ 11(c)), FRANZONE texted Wealth Manager-1 an explanation as to why FRANZONE did not have audited financials.

18. Based on my training and experience, I also know that, where computers, cellphones, and other electronic devices are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because:

- Electronic files can be stored on a hard drive for years at little or no cost and users thus have little incentive to delete data that may be useful to consult in the future.

- Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is "deleted" on a computer, cellphones, or other electronic devices, the data contained in the file does not actually disappear, but instead remains on the hard drive, in "slack space," until it is overwritten by new data that cannot be stored elsewhere on the device. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or "cache," which is only overwritten as the "cache" fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was created

or viewed than on a particular user's operating system, storage capacity, and user habits.

- In the event that a user changes devices, the user will typically transfer files from the old device to the new device, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash memory cards, CD-ROMs, or portable hard drives.

19. In addition to there being probable cause to believe that computers, cellphones, and/or other electronic devices will be found at the Subject Premises that contain evidence of the Subject Offenses, there is also probable cause to believe that these devices constitute instrumentalities of the Subject Offenses because they were used to communicate with victims.

20. Based on the foregoing and on the facts set forth in the Complaint, including FRANZONE's use of email and text message communications in connection with the operation of FF Fund (*see id.* ¶¶ 5-7, 11), I respectfully submit there is probable cause to believe that FRANZONE and others engaged in wire fraud and securities fraud offenses in the operation of FF Fund, in violation of Title 15, United States Code, Sections 78j(b) & 78ff, 17 C.F.R. Section 240.10b-5 (securities fraud); and Title 18, United States Code, Sections 1343 (wire fraud) and 2 (aiding and abetting), and that evidence of this criminal activity is likely to be found on the Subject Devices, and that the Subject Devices also are instrumentalities of the Subject Offenses.

IV. Procedures for Searching ESI

A. Review of ESI

21. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant that was created, modified, sent, received, or accessed between January 1, 2014 through the date of the execution of the warrant.

22. In conducting this review, law enforcement may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by "opening" or reading the first few "pages" of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

23. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement may need to conduct a complete review of all the ESI from the Subject Devices to locate all data responsive to the warrant.

B. Return of the Subject Devices

24. If the Government determines that the Subject Devices are no longer necessary to retrieve and preserve the data on the device, and that the Subject Devices are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return the Subject Device, upon request. Electronic data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the

offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

V. Conclusion and Ancillary Provisions

25. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

__S/ by the Court with permission__
EDWARD F. GANNON
Postal Inspector
United States Postal Inspection Service

Sworn to before me by
reliable electronic means
on _21_ of May 2021

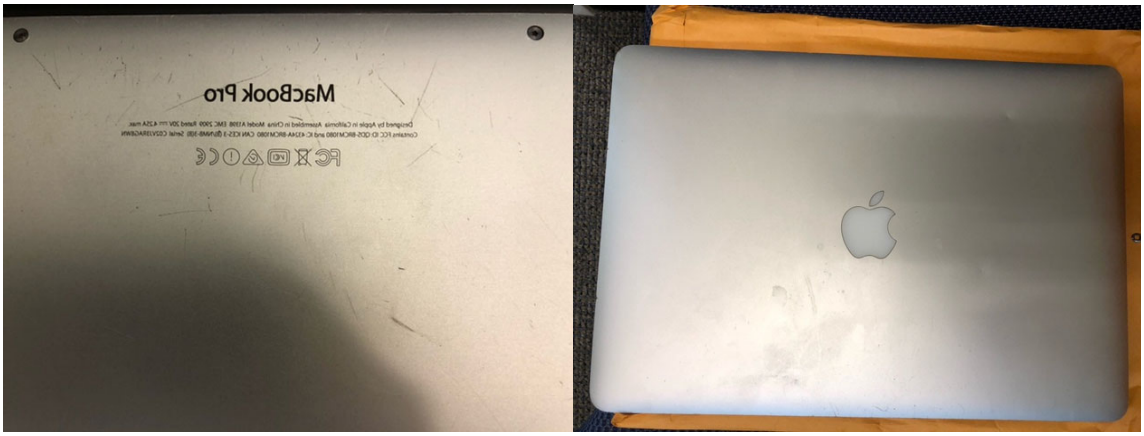
_____
HON. ROBERT W. LEHRBURGER
UNITED STATES DISTRICT JUDGE

Attachment A

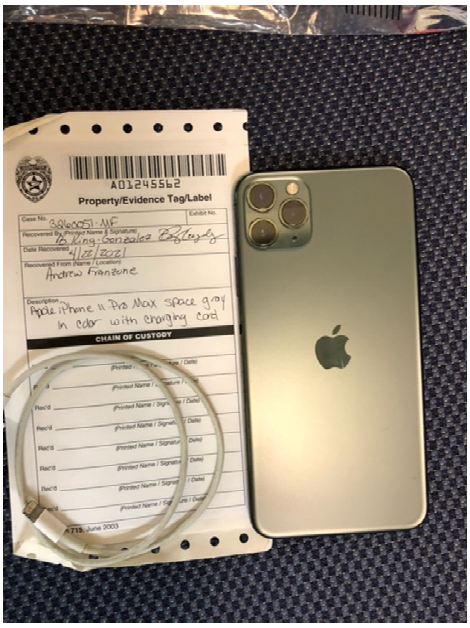
I. Devices Subject to Search and Seizure

The devices that are the subject of this search and seizure warrant (the "Subject Devices") are described as follows:

a. A silver Apple MacBook Pro with serial number C02VJ3RAG8WN ("Subject Device-1"), as depicted in the below photographs:

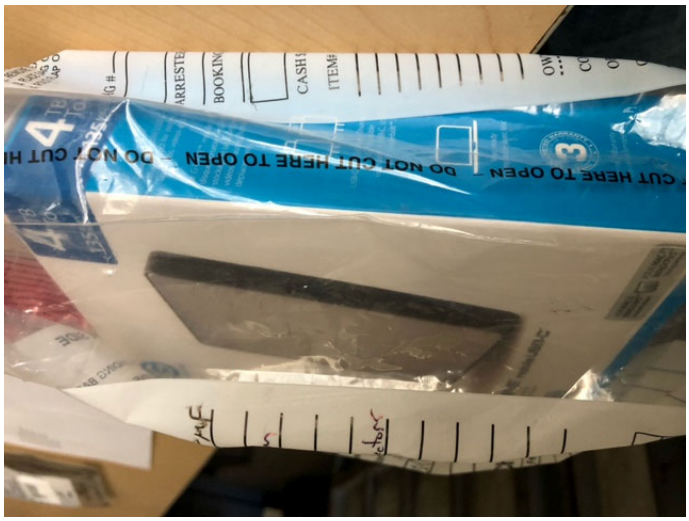


b. An Apple iPhone 11 Pro Max space gray in color ("Subject Device-2"), as depicted in the below photograph:



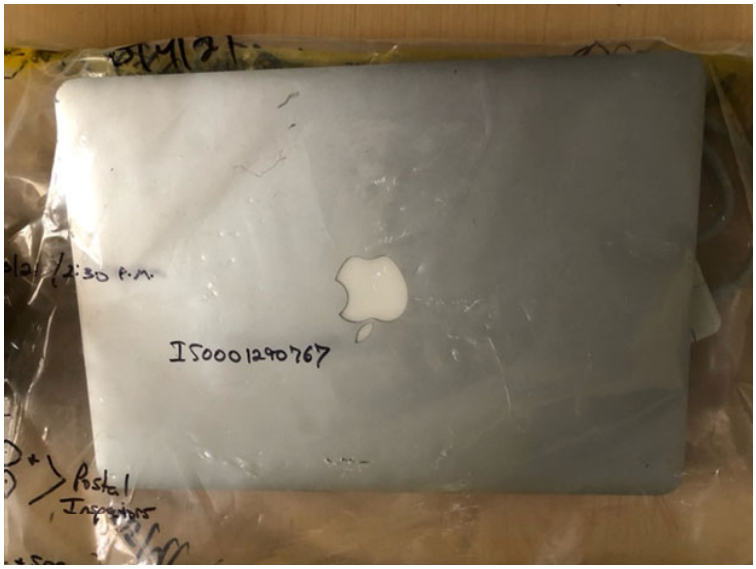
c. An Apple iPhone and Box with power cord ("Subject Device-3"), as depicted in the below photographs:

d. A 4 terabyte G Drive Hard drive with serial number WX11D79FHD7U ("Subject Device-4"), as depicted in the below photograph:



e. A 2 terabyte G Drive Hard drive with serial number WX11E29C1N68 ("Subject Device-5"), as depicted in the below photograph:

f. An Apple MacBook Air with serial number C1MPWM68G940 ("Subject Device-6"), as depicted in the below photograph:



II. Review of ESI on the Subject Devices

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the

government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the Subject Devices that was created, modified, sent, received, or accessed between January 1, 2012 through the date of the execution of the warrant for evidence, fruits, and instrumentalities of violations of Title 15, United States Code, Sections 78j(b) & 78ff, 17 C.F.R. Section 240.10b-5 (securities fraud); and Title 18, United States Code, Sections 1343 (wire fraud) and 2 (aiding and abetting) (collectively, the "Subject Offenses") relating to a fraud scheme involving FF Fund I L.P. (the "FF Fund Scheme"), described as follows:

1. Evidence concerning the identities or locations of those persons with access to, control over, or ownership of the Subject Devices.

2. Evidence concerning the identity or location of, and communications with, potential co-conspirators and/or victims of the FF Fund Scheme.

3. Evidence, including documents and communications, reflecting the state of mind of participants in the Subject Offenses, including communications among members of the scheme and any communications reflecting false (purportedly exculpatory) explanations of any participant's involvement in the Subject Offenses.

4. Evidence, including documents and communications, of motive for the Subject Offenses.

5. Evidence of other individuals who may have assisted the FF Fund Scheme, ledgers, delivery and payment records, accounting records, data that was sent or received, notes as to how the criminal conduct was achieved, records of discussions about the crime, promotional materials, and other records reflecting the planning and execution of the FF Fund Scheme.

6. Evidence concerning the location of proceeds of the FF Fund Scheme, including documentation of financial transactions, bank statements, checks, books, records, invoices, payment receipts, money orders, cashier's checks, bank checks, safe deposit box keys, money wrappers, filed and non-filed income tax records, credit card receipts, credit card statements, minute books and other items evidencing the obtaining, secreting, transferring, and/or concealment of assets and the obtaining, secreting, transferring, concealment, and/or expenditure of money as part of the FF Fund Scheme.

7. Evidence revealing the passwords or other information of other participants in the Subject Offenses needed to access the user's computer, smartphone, or other devices or accounts that may contain evidence of the Subject Offenses.

8. Documents and other materials identifying the location of other evidence of the Subject Offenses.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;

- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;

- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and

- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the device was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Section II of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.